

REMARKS

This is a full and timely response to the outstanding non-final Office Action mailed November 20, 2003.

As an initial matter, Applicants thank the Examiner for such a careful and meticulous review of the application. However, for at least the reasons set forth below, Applicants respectfully request reconsideration and allowance of the application and pending claims.

I. Claim Objections

Claim 21 has been objected to because of the following formality: "The system claim 18" should be changed to "The system of claim 18."

Claim 21 has been directly amended to overcome the objection. Applicants respectfully note that the amendment is purely for cosmetic purposes and is intended to limit neither the scope of claim 21 nor its available equivalents.

II. Claim Rejections - 35 U.S.C. § 102(e)

A. Statement of the Rejection

Claims 1-3 have been rejected under 35 U.S.C. § 102(e) as being anticipated by Kuroda ("Kuroda," U.S. Pat. No. 5,935,248).

The rejection states that Kuroda discloses Applicants' invention as recited in the above-identified claims. Applicants respectfully traverse this rejection.

B. Discussion of the Rejection

"Anticipation requires the disclosure in a single prior art reference of *each element* of the claim under consideration." W. L. Gore & Associates, Inc. v. Garlock, Inc., 721 F.2d 1540, 1554, 220 U.S.P.Q. 303, 313 (Fed. Cir. 1983)(emphasis added). Therefore, every claimed feature of the claimed invention must be represented in the applied reference to constitute a proper rejection under 35 U.S.C. § 102(e).

In the present case, not every feature of the claimed invention is represented in the Kuroda reference.

Claim 1 recites:

1. (Original) A method for applying adaptive security to a data stream, comprising the steps of:

identifying a desired security level range and a desired actual security level which falls within the desired security level range for communicating a data stream from a send host to a receive host;

determining an actual security level in the receive host ***based upon the availability of a number of security processor operations***;

communicating the actual security level from the receive host to the send host;

generating a plurality of data packets associated with the data stream in the send host, the data packets having an authentication header including the desired security level range and the actual security level;

reallocating computing resources at the receive host if data packets cannot be verified at the desired actual security level with a current allocation of resources; and

verifying the data packets at the actual security level, the actual security level being within the desired security level range.

(emphasis supplied).

The Office Action alleges that the cited portion of Kuroda teaches the step of "determining an actual security level in the receive host based on the availability of a number of security processor operations."

However, contrary to the position set forth in the Office Action, the cited portion of Kuroda does not teach the determination of an actual security level in the receive host based on the availability of a number of security processor operations. In fact, the cited portion of Kuroda makes no mention of the availability of a number of security processor operations. Specifically, the cited portions of Kuroda teach:

In accordance with the first security level control apparatus 10 of the present invention, the following operations are carried out. First, the security level of the communication party recognized by the security level recognizing unit 11 is set as the security level for the security level control apparatus 10.

Second Security Level Control Apparatus 10

To solve the above-described second problem, a second security level control apparatus 10 of the present invention is arranged as follows (corresponding to claim 2). FIG. 1 is a schematic block diagram for showing a basic idea of the security level control apparatus 10 according to the present invention.

That is, the security level apparatus 10 for controlling a security level of a communication executed between communication parties is arranged by a security level recognizing unit 11, a security level converting table unit 12, a security level reading unit 13, and a security level setting unit 14.

(Security Level Recognizing Unit 11)

The security level recognizing apparatus 11 may recognize a security level notified from communication destination (communication party).

Kuroda at column 3, line 62 through column 4, line 18.

As seen above, the cited portion of Kuroda makes no mention of determining an actual security level based on the availability of a number of security processor operations. Other portions of Kuroda indicate that the security level in Kuroda is determined by Kuroda's security level converting table unit in conjunction with a security level notified

from a communication destination (see, *e.g.*, Kuroda at column 6). As such, it appears that claim 1 is patently distinguishable from the teachings of Kuroda.

In the absence of any mention of a number of security processor operations, it is axiomatic that Kuroda cannot suggest the determining of an actual security level based on the availability of the number of security processor operations. In that regard, Kuroda does not render claim 1 obvious.

Due to these shortcomings of the Kuroda reference, Applicants respectfully assert that Kuroda neither anticipates claim 1, nor render it obvious. Therefore, Applicants respectfully request that the rejection of claim 1 be withdrawn.

Claims 2-10 depend, either directly or indirectly, from independent claim 1. Applicants submit that claims 2-10 are allowable for at least the reason that they depend, either directly or indirectly, from allowable base claims. As such, Applicants respectfully request that the rejection of claims 2-10 also be withdrawn.

III. Claim Rejections - 35 U.S.C. § 103(a)

A. Statement of the Rejection

Claims 4-31 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Kuroda in view of Jurkevich, et al. ("Jurkevich", U.S. Pat. No. 5,164,938). Applicants respectfully traverse this rejection.

B. Discussion of the Rejection

Claims 11 recites:

11. (Original) A method for communicating and applying adaptive security to a data stream comprising a plurality of data packets, comprising the steps of:

identifying a desired security level range and a desired actual security level which falls within the desired security level range for the data stream to be received by a host;

determining the *availability of a number of security processor operations* at the host;

reallocating computing resources at the host if the data stream cannot be verified at the desired actual security level;

reallocating communication resources if there are insufficient computing resources available for reallocation at the host; and

verifying the data packets at the actual security level, the actual security level being within the desired security level range.

(emphasis supplied).

Claims 18 recites:

18. (Original) A system for facilitating data communication to a host with adaptive security, comprising:

means for determining whether a desired actual security level for a transmitted data stream falls within a desired security level range;

means for determining the *availability of a number of security processor operations* at the host;

means for reallocating computing resources at the host if the data stream cannot be verified at the desired actual security level; and

means for reallocating communication resources if there are insufficient computing resources available for reallocation at the host.

(emphasis supplied).

Claims 25 recites:

25. (Original) A computer program embodied on a computer-readable medium for facilitating data communication to a host with adaptive security, comprising:

logic configured to determine whether a desired actual security level for a transmitted data stream falls within a desired security level range;

logic configured to determine the *availability of a number of security processor operations* at the host;

logic configured to reallocate computing resources at the host if the data stream cannot be verified at the desired actual security level; and logic configured to reallocate communication resources if there are insufficient computing resources available for reallocation at the host. (emphasis supplied).

While claims 11, 18, and 25 are of varying scope and, hence, do not stand or fall together, each of claims 11, 18, and 25 requires the "availability of a number of security processor operations." As discussed with reference to claim 1, Kuroda is wholly lacking in any teaching or suggestion related to the availability of a number of security processor operations. In that regard, Kuroda neither anticipates nor renders obvious claims 11, 18, or 25.

Insofar as Kuroda is deficient for failing to teach or suggest the availability of a number of security processor operations, it is axiomatic that Jurkevich, in combination with Kuroda, will necessarily suffer from the same deficiency. In other words, Jurkevich, which also does not teach the availability of a number of security processor operations, cannot cure Kuroda, which is deficient for failing to teach the availability of a number of security processor operations.

Since Jurkevich cannot cure the deficiency of Kuroda, Applicants respectfully assert that the combination of Jurkevich with Kuroda cannot render Applicants' claims obvious. Therefore, Applicants respectfully request that the rejection of claims 11, 18, and 25 be withdrawn.

Claims 12-17 depend, either directly or indirectly, from independent claim 11; claims 19-24 depend, either directly or indirectly, from independent claim 18; and claims 26-31 depend, either directly or indirectly, from independent claim 25. Applicants respectfully submit that, insofar as these claims depend, either directly or indirectly, from

allowable base claims, for at least this reason, claims 12-17, 19-24, and 26-31 are allowable over the cited references. Thus, Applicants respectfully request that the rejection of claims 12-17, 19-24, and 26-31 also be withdrawn.

III. Double Patenting Rejections


Claims 1-3, 11-12, 17-20, 25-27, and 31 have been provisionally rejected under 35 U.S.C. § 101 as claiming the same invention as that of claims 1-31 of U.S. Patent No. 6,510,349.

Although Applicants do not agree with the basis for the rejection, Applicants submit herewith a terminal disclaimer disclaiming any term that would extend beyond the term of U.S. Patent No. 6,510,349. In view of this terminal disclaimer, Applicants respectfully submit that the rejection is moot.

CONCLUSION

Applicants respectfully submit that pending claims 1-31 are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (770) 933-9500.

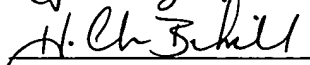
Respectfully submitted,



Sam S. Han
Registration No. 51,771

**THOMAS, KAYDEN,
HORSTEMEYER & RISLEY, L.L.P.**
Suite 1750
100 Galleria Parkway N.W.
Atlanta, Georgia 30339
(770) 933-9500

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, postage prepaid, in an envelope addressed to: Assistant Commissioner for Patents, Alexandria, Virginia 22313-1450, on

January 7, 2004


Signature :